TÜV TRUST IT
TÜV AUSTRIA Group

Zertifizierung

Zertifizierung nach ISO 27001 auf der Basis von IT Grundschutz

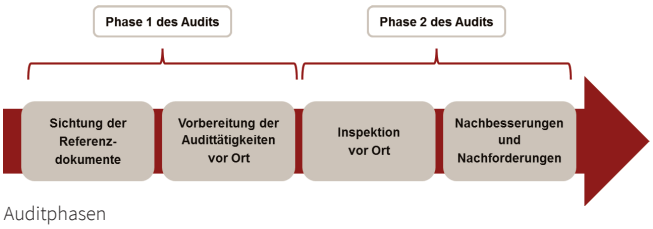
Informationen sind die Basis für den Ablauf von Geschäfts- und Produktionsprozessen sowie für die Kommunikation mit Kunden und Partnern. Um die Unternehmensinformationen in angemessener Weise zu schützen, bedarf es wirksamer Prozesse, wie sie in einem Informationssicherheitsmanagementsystem (ISMS) abgebildet werden.

Oberstes Ziel des ISMS ist es, Informationen vor Verlust der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität zu schützen. Der Aufbau eines ISMS umfasst daher im Wesentlichen Prozesse zur Analyse und Bewertung von Risiken, die sich durch den IT-Betrieb ergeben sowie der Auswahl und Überwachung geeigneter Sicherheitsmaßnahmen, um diese Risiken angemessen zu behandeln. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für den Aufbau eines entsprechenden ISMS nach ISO 27001 auf der Basis von IT Grundschutz eigene Standards entwickelt, die die Vorgehensweise detailliert aufzeigen.

Ist ein ISMS nach diesen Vorgaben aufgebaut, steht als nächster möglicher Schritt die Zertifizierung an. Diese Zertifizierung wird beim BSI beantragt, das gleichzeitig als Zertifizierungsstelle agiert. Für die Durchführung der Zertifizierungsaudits ist die Teilnahme mindestens eines Auditors verpflichtend, der durch das BSI zum ISO 27001 Auditteamleiter für Audits auf der Basis von IT-Grundschutz berufen ist. Die TÜV TRUST IT verfügt über eine Reihe erfahrener und vom BSI berufener Auditoren, die diese Zertifizierung durchführen können.

Vorgehensweise

Das Zertifizierungsaudit nach ISO 27001 auf der Basis von IT-Grundschutz erfolgt in vier Teilschritten, die im Folgenden näher beschrieben werden:



Auditphasen

Sichtung der Referenzdokumente

Die folgenden Dokumente werden auf Qualität, Aktualität, Vollständigkeit und Sinnhaftigkeit überprüft:

- Richtlinien für die Informationssicherheit
- Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung des Informationsverbunds
- Ergebnis des Basis-Sicherheitschecks
- Ergänzende Sicherheitsanalyse
- Risikoanalyse
- Risikobehandlungsplan

Vorbereitung der Audittätigkeit vor Ort

Der Auditor erstellt einen Prüfplan und legt die Prüfbausteine fest.

Inspektion vor Ort

Anhand von Stichproben wird überprüft, ob der dokumentierte Umsetzungsstatus den Gegebenheiten entspricht. Hierbei wird die Wirksamkeit des Managementsystems für die Informationssicherheit hinterfragt und dafür Interviews mit den entsprechenden Verantwortlichen geführt. Zudem erfolgt

Zertifizierung

eine Verifikation des Netzplans, der Liste der IT-Systeme, des Basis-Sicherheitschecks und der Umsetzung der zusätzlichen Maßnahmen aus der ergänzenden Risikoanalyse.

Nachbesserungen und Nachforderungen

Bei der ersten Sichtung der Referenzdokumente sowie der Inspektion vor Ort können sich in manchen Fällen Abweichungen ergeben, die sachgerecht behoben werden müssen. Darüber werden Sie rechtzeitig informiert, sodass diese in einer angemessenen Frist aufgearbeitet werden können. Die Abweichungsliste und die Nachbesserungsfrist für die Empfehlungen und Korrekturmaßnahmen werden im Auditbericht dokumentiert. Somit wird bereits vor Phase 2 des Audits die Möglichkeit gegeben, die ermittelten Abweichungen aus Phase 1 zu beheben.

Die Ergebnisse der Zertifizierungsprüfungen werden schließlich in einem umfassenden Abschlussbericht erfasst und dem BSI eingereicht. Bei erfolgreichem Abschluss der beiden Auditphasen empfehlen unsere Auditoren dem BSI die Erteilung des Zertifikats, welches nach positiver Prüfung des Berichts durch die Zertifizierungsstelle des BSI ausgestellt wird. Zur Aufrechterhaltung der dreijährigen Gültigkeit des Zertifikats sind jährliche Überwachungsaudits sowie im dritten Jahr eine Re-Zertifizierung erforderlich.

Ihr Nutzen

- Beleg gegenüber Ihren Kunden und Geschäftspartnern, dass Ihr Sicherheitsmanagement optimal aufgestellt ist
- Dauerhafte Verbesserung der ISMS-Prozesse durch regelmäßige Überprüfung
- Aufdeckung von Schwachstellen und Herausstellung von Verbesserungspotenzialen
- Vermeidung unerwarteter Kosten aus Sicherheitsvorfällen
- Qualifizierte ISO 27001 Auditteamleiter, die durch das BSI für Audits auf der Basis von IT-Grundschutz berufen sind

TÜV TRUST IT GmbH
Unternehmensgruppe TÜV AUSTRIA

Waltherstraße 49–51
D-51069 Köln
Tel.: +49 (0)221 969789 - 0
Fax: +49 (0)221 969789 -12

TÜV TRUST IT
TÜV AUSTRIA GmbH

TÜV AUSTRIA-Platz 1
A-2345 Brunn am Gebirge
Tel.: +43 (0) 5 0454 - 1000
Fax: +43 (0) 5 0454 - 76245

info@tuv-austria.com
www.it-tuv.com